

CLAIMS

1. A method for passive probing forwarded one or more TCP communication sessions between a client and a server, said method comprising the steps of:
- a. receiving forwarded data packets corresponding to said TCP communication sessions;
 - b. ordering said received data packets and reconstructing session content for each of said one or more sessions; and
 - c. forwarding said reconstructed session content to an external entity.
2. A method as per claim 1, wherein at least one of said communication sessions is encrypted, and, for each encrypted session, said method additionally comprising the steps of:
- d. identifying, prior to said forwarding step, an encryption scheme and a session key from said reconstructed content; and
 - e. decrypting said session content based upon said identified encryption scheme and said session key,
- wherein said forwarded session content in (c) is said decrypted session content.

3. A method as per claim 2, wherein said at least one encrypted communication session is encrypted via the secure socket layer (SSL) protocol.

4. A method as per claim 1, wherein said method further comprises the step of filtering said reconstructed session content to isolate information pertinent to said external entity, and in step (c), forwarding said isolated information pertinent to said external entity.

5. A method as per claim 4, wherein said isolated content represents unencrypted communications from said client.

6. A method as per claim 4, wherein said isolated content represents unencrypted communications from said server.

7. A method as per claim 1, wherein said external entity is a network data analysis application.

8. A passive secure socket layer (SSL) probe working in conjunction with network equipment and an external entity, said network equipment forwarding a copy of encrypted data in a secure communication session between a client and a server to said SSL probe, said SSL probe comprising:

a. a receiver receiving data packets corresponding to said forwarded encrypted data from said network equipment, ordering said received data packets for a TCP session, and reconstructing the session content;

5 b. a symmetric session key generator receiving said session content for said TCP session from said receiver, identifying SSL handshake information from said session content, and identifying an encryption scheme and a symmetric session key using said SSL handshake information;

c. a decrypter decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key; and

10 d. a forwarder forwarding said decrypted session content to said external entity.

9. A passive secure socket layer (SSL) probe as in claim 8, wherein said forwarder further comprises a filter filtering said generated unencrypted session content to isolate
15 information pertinent to said external entity, and said forwarder forwarding said isolated information pertinent to said external entity.

10. A passive secure socket layer (SSL) probe as in claim 8, wherein said forwarder further comprises a filter filtering said generated unencrypted session content to isolate

unencrypted communications from said client, and said forwarder forwarding said isolated
unencrypted communications from said client.

11. A passive secure socket layer (SSL) probe as in claim 8, wherein said external
5 entity is a network data analysis application.

12. A passive secure socket layer (SSL) probe as in claim 8, wherein said forwarder
further comprises a filter filtering said generated unencrypted session content to isolate
unencrypted communications from said server, and said forwarder forwarding said isolated
10 unencrypted communications from said server.

13. A method for passive decryption of encrypted data, said method as implemented
in a passive secure socket layer (SSL) probe comprising the steps of:

a. receiving data packets corresponding to said encrypted data, said
15 encrypted data forwarded to said SSL probe from network equipment, said network
equipment replicating encrypted data in secure communication sessions between a
client and a server, and said forwarded data corresponding to said secure
communication sessions;

b. ordering said received data packets of a TCP session and reconstructing
20 the session content;

- c. identifying SSL handshake information from said session content;
- d. identifying an encryption scheme and a symmetric session key using said identified SSL handshake information;
- e. decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key; and
- f. forwarding said decrypted session content to an external entity.

14. A method for passive decryption of encrypted data, as in claim 13, wherein said method further comprises the step of filtering said decrypted session content to isolate information pertinent to said external entity, and, in step (f), forwarding said isolated information pertinent to said external entity.

15. A method for passive decryption of encrypted data, as in claim 13, wherein said method further comprises the step of filtering said decrypted session content to isolate unencrypted communications from said client, and, in said step (f), forwarding said isolated unencrypted communications from said client.

16. A method for passive decryption of encrypted data, as in claim 13, wherein said method further comprises the step of filtering said decrypted session content to isolate

unencrypted communications from said server, and, in said step (f), forwarding said isolated unencrypted communications from said server.

17. A method for passive decryption of encrypted data, as in claim 13, wherein said external entity is a network data analysis application.

18. An article of manufacture comprising a computer usable medium having computer readable program code embodied therein providing passive decryption of encrypted data, said medium comprising:

a. computer readable program code aiding in receiving data packets corresponding to said encrypted data, said encrypted data forwarded to a Secure Sockets Layer (SSL) probe from network equipment, said network equipment replicating encrypted data in secure communication sessions between a client and a server, and said forwarded data corresponding to said secure communication sessions;

b. computer readable program code ordering said received data packets of a TCP session and reconstructing the session content;

c. computer readable program code identifying SSL handshake information from said session content;

d. computer readable program code identifying an encryption scheme and a symmetric session key using said identified SSL handshake information;

e. computer readable program code decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key; and

f. computer readable program code aiding in forwarding said decrypted session content to an external entity.

19. An article of manufacture, as per claim 18, wherein said medium further comprises computer readable program code filtering said decrypted session content to isolate information pertinent to said external entity, and, in step (f), computer readable program code aiding in forwarding said isolated information pertinent to said external entity.

20. An article of manufacture, as in claim 18, wherein said medium further comprises computer readable program code filtering said decrypted session content to isolate unencrypted communications from said client, and, in step (f), computer readable program code aiding in forwarding said isolated unencrypted communications from said client.

21. An article of manufacture, as in claim 18, wherein said medium further comprises computer readable program code filtering said decrypted session content to isolate unencrypted

communications from said server, and, in step (f), computer readable program code aiding in forwarding said isolated unencrypted communications from said server.

22. A method for passive decryption of encrypted data, said method as implemented
5 in a passive secure socket layer (SSL) probe comprising the steps of:

receiving data packets forwarded to said SSL probe from a network equipment,
said network equipment replicating data in a communication session between a client and a
server;

in said received data packets, selecting and isolating data packets corresponding to
10 encrypted communication sessions;

ordering data packets in said isolated data packets of a TCP session and
reconstructing session content;

identifying SSL handshake information from said session content;

identifying an encryption scheme and a symmetric session key using said
15 identified SSL handshake information;

decrypting said session content, said decryption based upon said identified
encryption scheme and said identified symmetric key;

filtering said decrypted session content to isolate information pertinent to said
external entity; and

20 forwarding said filtered information pertinent to said external entity.

23. A method as per claim 22, wherein said step of selecting data packets
corresponding to encrypted communication sessions is based upon any of the following selection
criteria: IP address of the server, TCP port number of the server, client network range, or an
5 identifier in a data packet.

24. A method as per claim 22, wherein said external entity is a network data analysis
application.

10 25. A passive secure socket layer (SSL) probe working in conjunction with network
equipment and an external entity, said network equipment forwarding a copy of encrypted data in
a secure communication session between a client and a server to said SSL probe, said SSL probe
comprising:

15 a receiver receiving data packets corresponding to said forwarded encrypted data
from said network equipment, ordering said received data packets of a TCP session and
reconstructing session content;

a symmetric session key generator receiving said session content from said
receiver, identifying SSL handshake information from said session content, and identifying an
encryption scheme and a symmetric session key using said SSL handshake information;

a decrypter decrypting said session content, said decryption based upon said identified encryption scheme and said identified symmetric key;

a filter isolating information pertinent to said external entity via filtering said decrypted session content; and

5 a forwarder forwarding said isolated information pertinent to said external entity.

26. A passive secure socket layer (SSL) probe, as per claim 25, wherein said external entity is a network data analysis application.

10 27. Network equipment facilitating the flow of encrypted data in a secure communication session between a client and a server, said network equipment comprising:

a receiver receiving encrypted data packets corresponding to said secure communication session, copying data packets corresponding to said secure session, and for each secure session: ordering said copied data packets, and reconstructing the session content;

15 a session key generator receiving said reconstructed session content from said receiver, identifying SSL handshake information from said session content, and identifying an encryption scheme and a session key using said SSL handshake information;

a decrypter decrypting said session content, said decryption based upon said identified encryption scheme and said identified session key; and

a forwarder forwarding said received encrypted data packets to its intended destination and forwarding said decrypted session content to an external entity.

28. Network equipment as per claim 27, wherein said external entity is a network data analysis application.

29. Network equipment as per claim 27, wherein said forwarder further comprises a filter filtering said decrypted session content to isolate information pertinent to said external entity, and said forwarder forwarding said isolated information pertinent to said external entity.

30. Network equipment as per claim 27, wherein said forwarder further comprises a filter filtering said decrypted session content to isolate unencrypted communications from said client, and said forwarder forwarding said isolated unencrypted communications from said client to said external entity.

31. Network equipment as per claim 27, wherein said forwarder further comprises a filter filtering said generated unencrypted session content to isolate unencrypted communications from said server, and said forwarder forwarding said isolated unencrypted communications from said server to said external entity.

32. A method for passive probing of forwarded TCP communication sessions between a client and a server, said method comprising the steps of:

receiving forwarded data packets corresponding to said TCP communication sessions; and

5 ordering said received data packets and reconstructing session content for each TCP session, and if at least one of said communication sessions is encrypted, then:

identifying an encryption scheme and a session key

using said reconstructed session content;

decrypting said session content, said decryption

10 based upon said identified encryption scheme and said identified session key; and

forwarding said decrypted session content to an

external entity; else

forwarding said reconstructed session content of to an external entity.

15